TITLE: METHOD AND APPARATUS FOR IMPLEMENTING PROCESS-BASED SECURITY IN A COMPUTER SYSTEM
INVENTORS: Vincent Alan Larsen

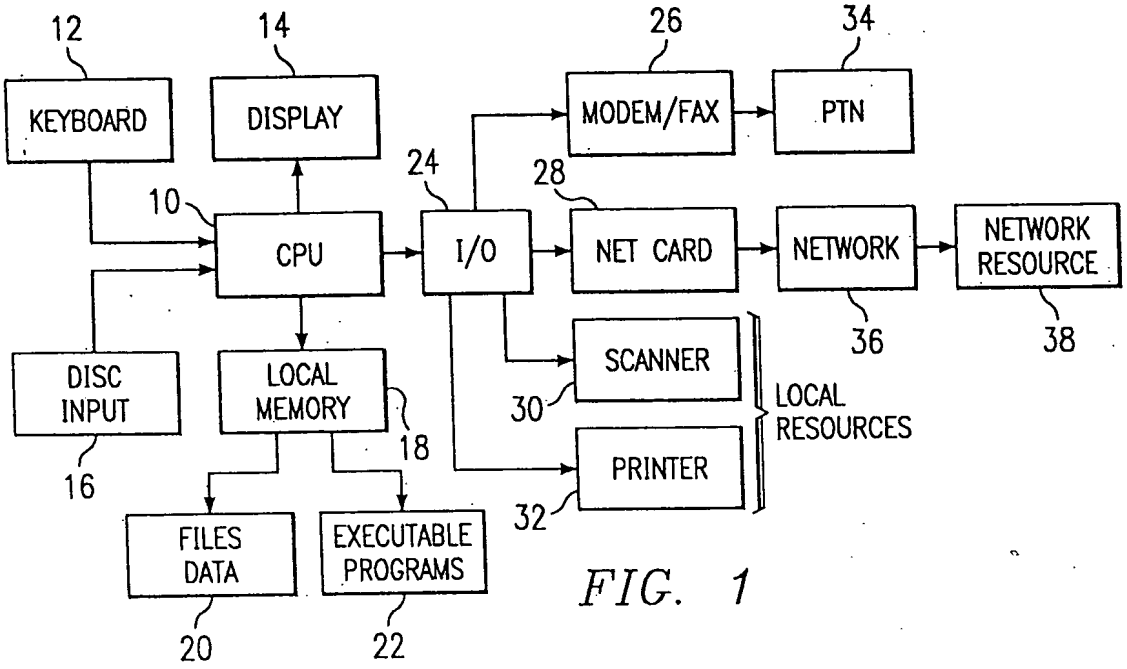


FIG. 1

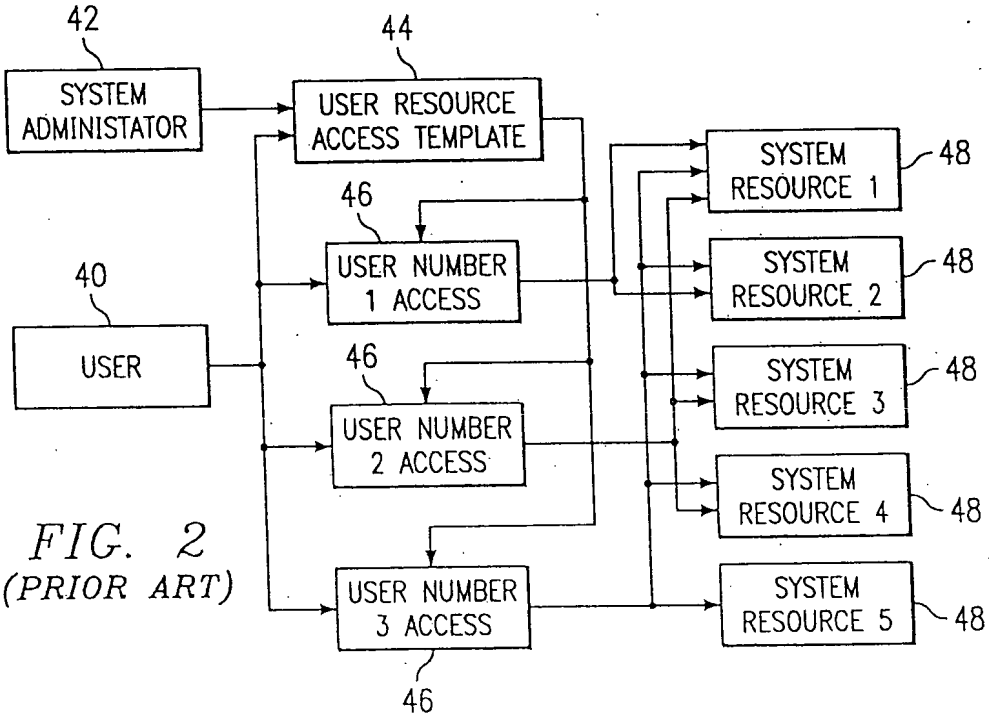
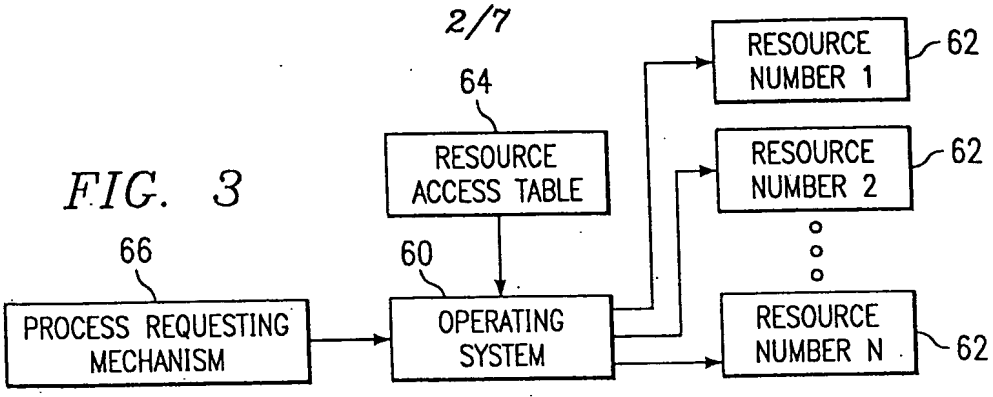


FIG. 2
(PRIOR ART)

FIG. 3


RESOURCE NUMBER 1
62
64
RESOURCE ACCESS TABLE
RESOURCE NUMBER 2
62
66
60
PROCESS REQUESTING MECHANISM
OPERATING SYSTEM
RESOURCE NUMBER N
62

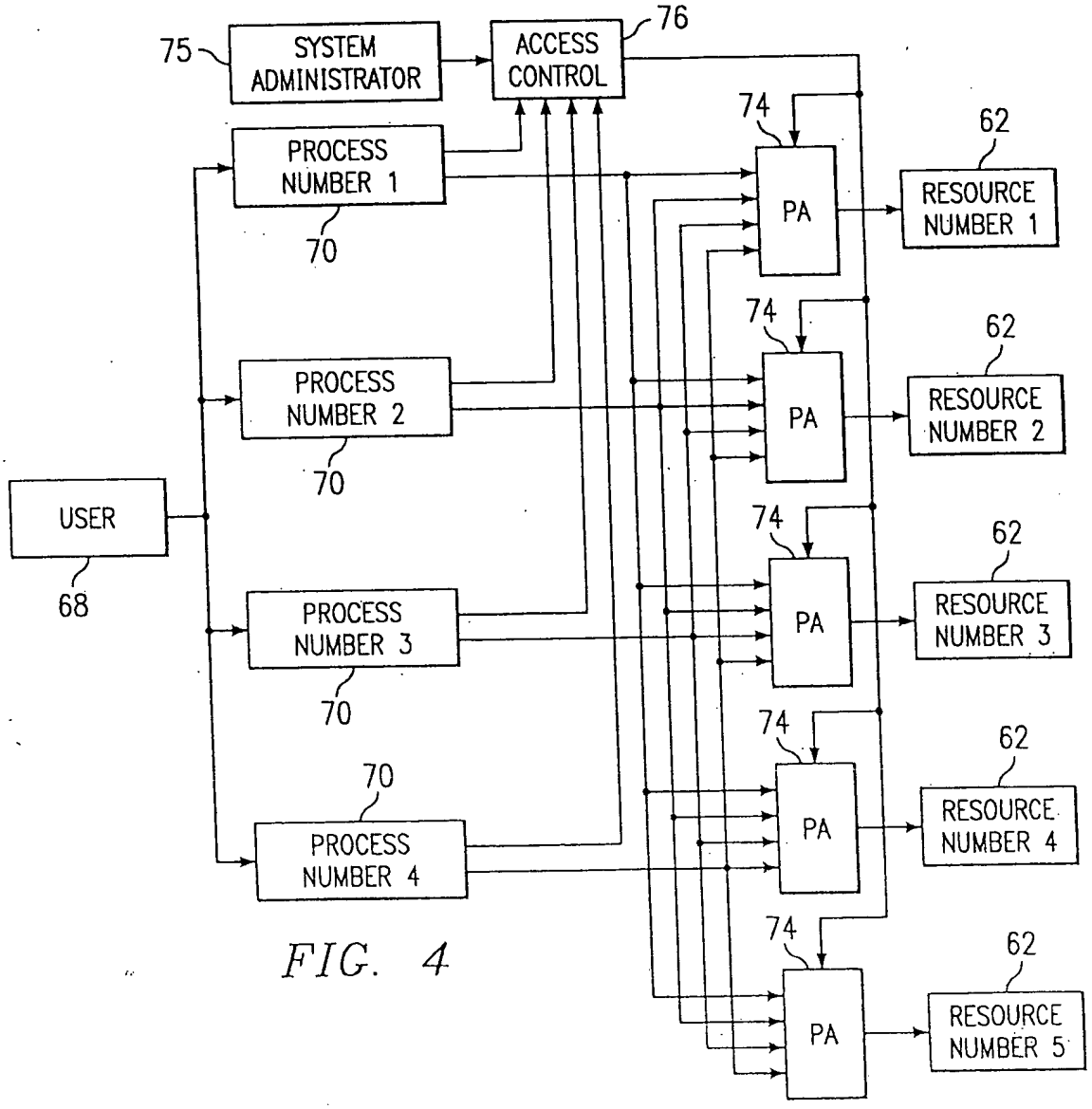

75
SYSTEM ADMINISTRATOR
ACCESS CONTROL
76
74
62
PROCESS NUMBER 1
70
PA
RESOURCE NUMBER 1
74
62
PROCESS NUMBER 2
70
PA
RESOURCE NUMBER 2
USER
68
74
62
PROCESS NUMBER 3
70
PA
RESOURCE NUMBER 3
74
62
70
PROCESS NUMBER 4
PA
RESOURCE NUMBER 4
74
62
PA
RESOURCE NUMBER 5

FIG. 4

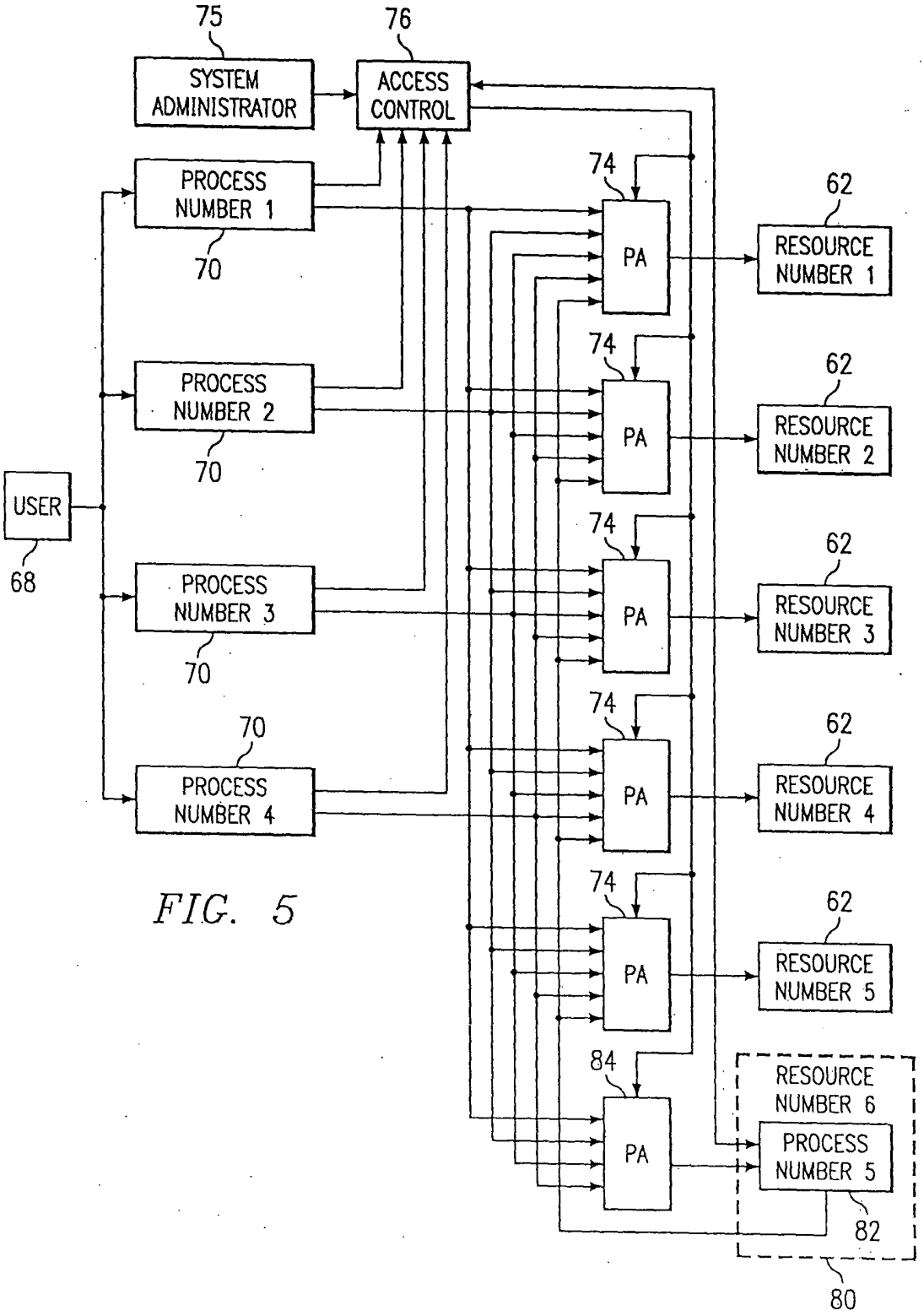

75
SYSTEM ADMINISTRATOR
76
ACCESS CONTROL
PROCESS NUMBER 1
70
PROCESS NUMBER 2
70
USER
68
PROCESS NUMBER 3
70
70
PROCESS NUMBER 4
74
PA
62
RESOURCE NUMBER 1
74
PA
62
RESOURCE NUMBER 2
74
PA
62
RESOURCE NUMBER 3
74
PA
62
RESOURCE NUMBER 4
74
PA
62
RESOURCE NUMBER 5
84
PA
RESOURCE NUMBER 6
PROCESS NUMBER 5
82
80

FIG. 5

FIG. 6

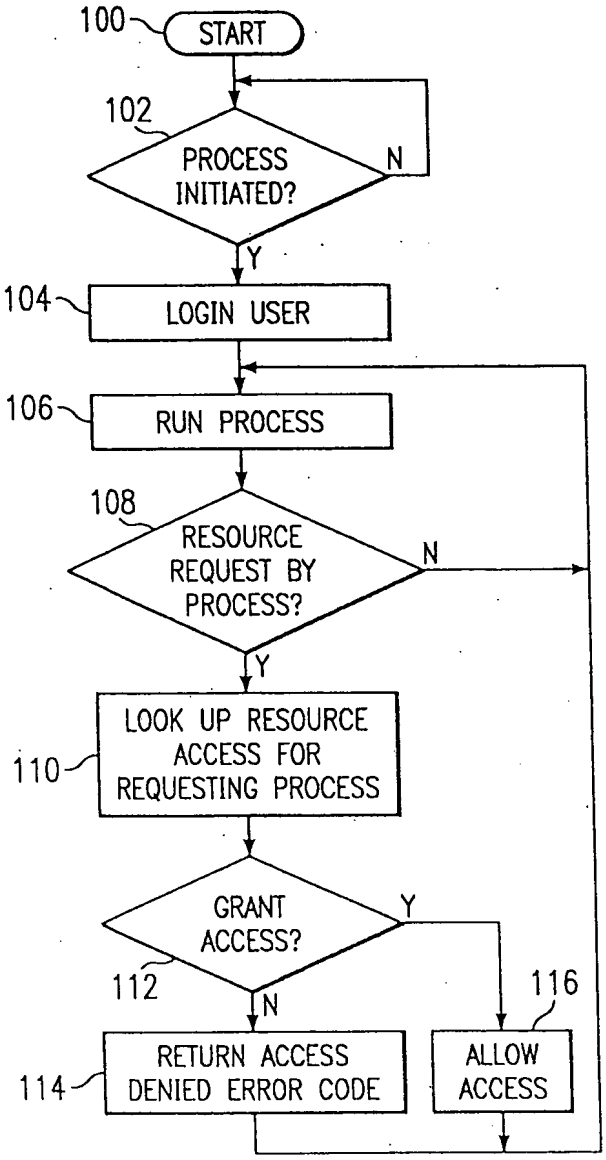

100
START
102
PROCESS INITIATED?
N
Y
104
LOGIN USER
106
RUN PROCESS
108
RESOURCE REQUEST BY PROCESS?
N
Y
110
LOOK UP RESOURCE ACCESS FOR REQUESTING PROCESS
GRANT ACCESS?
Y
112
N
116
114
RETURN ACCESS DENIED ERROR CODE
ALLOW ACCESS

FIG. 7

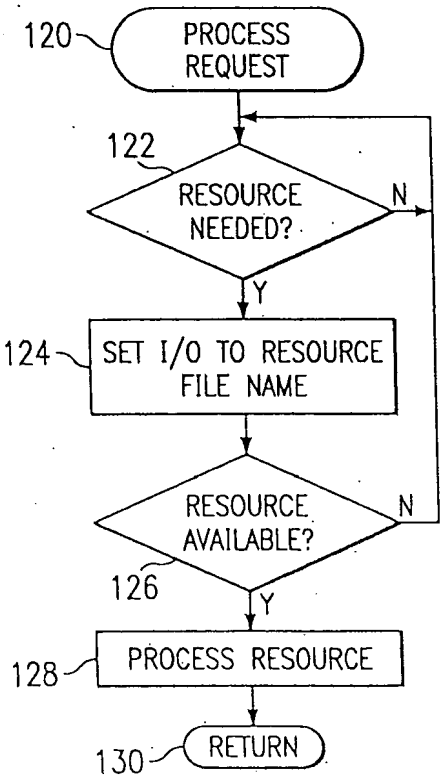

120
PROCESS REQUEST
122
RESOURCE NEEDED?
N
Y
124
SET I/O TO RESOURCE FILE NAME
RESOURCE AVAILABLE?
N
126
Y
128
PROCESS RESOURCE
130
RETURN

FIG. 8

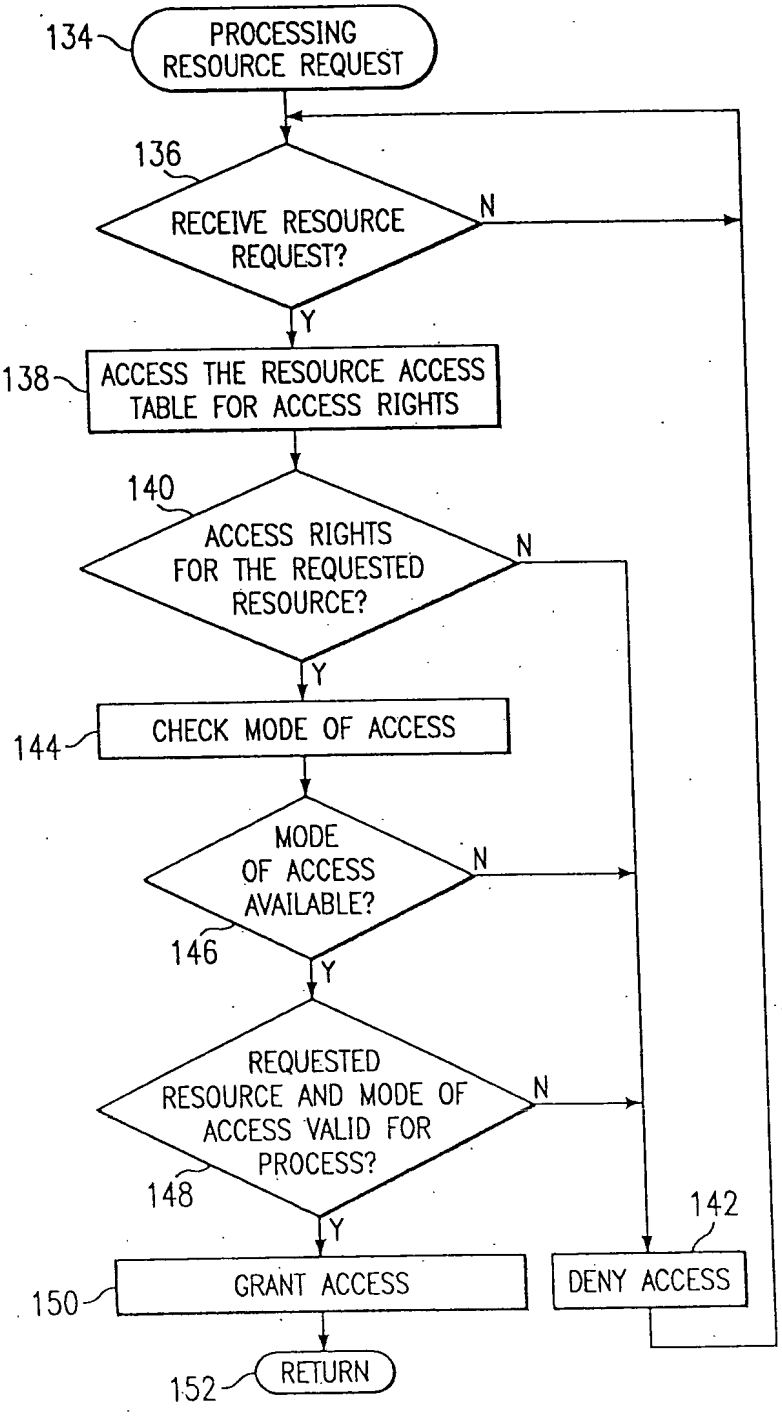

134
PROCESSING RESOURCE REQUEST
136
RECEIVE RESOURCE REQUEST?
N
Y
138
ACCESS THE RESOURCE ACCESS TABLE FOR ACCESS RIGHTS
140
ACCESS RIGHTS FOR THE REQUESTED RESOURCE?
N
Y
144
CHECK MODE OF ACCESS
MODE OF ACCESS AVAILABLE?
N
146
Y
REQUESTED RESOURCE AND MODE OF ACCESS VALID FOR PROCESS?
N
148
Y
142
GRANT ACCESS
DENY ACCESS
150
RETURN
152

FIG. 9

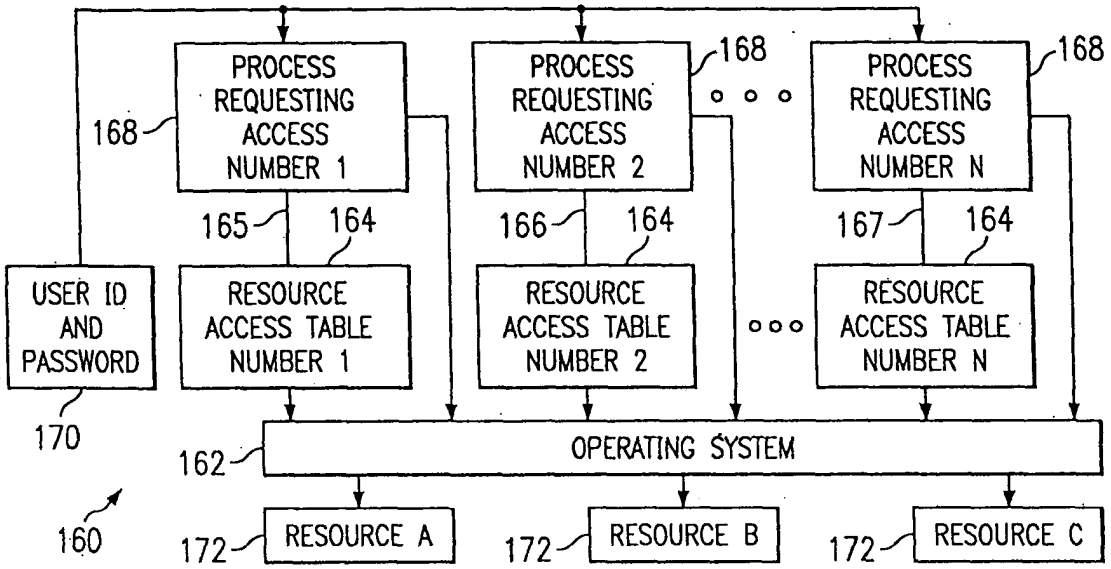

PROCESS REQUESTING ACCESS NUMBER 1
PROCESS REQUESTING ACCESS NUMBER 2
PROCESS REQUESTING ACCESS NUMBER N
168
168
168
165
164
166
164
167
164
USER ID AND PASSWORD
RESOURCE ACCESS TABLE NUMBER 1
RESOURCE ACCESS TABLE NUMBER 2
RESOURCE ACCESS TABLE NUMBER N
170
162
OPERATING SYSTEM
160
172
RESOURCE A
172
RESOURCE B
172
RESOURCE C

FIG. 10

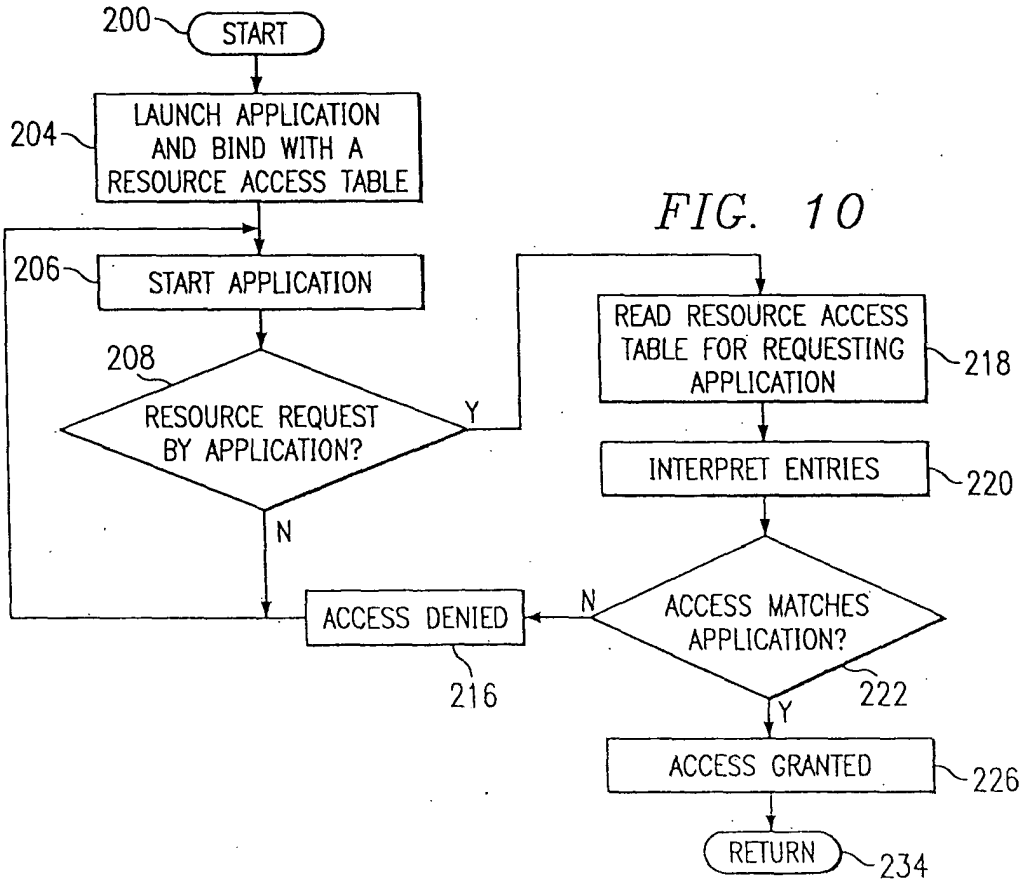
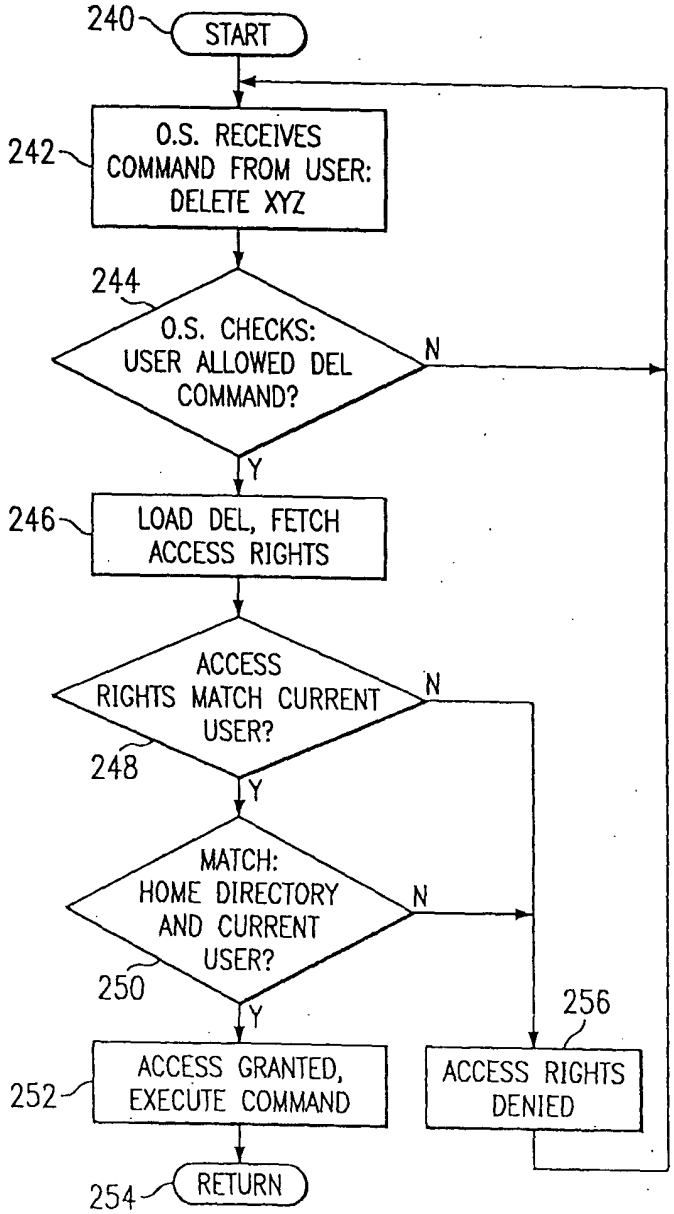

200
START
204
LAUNCH APPLICATION AND BIND WITH A RESOURCE ACCESS TABLE
206
START APPLICATION
208
RESOURCE REQUEST BY APPLICATION?
Y
N
ACCESS DENIED
216
READ RESOURCE ACCESS TABLE FOR REQUESTING APPLICATION
218
INTERPRET ENTRIES
220
ACCESS MATCHES APPLICATION?
N
222
Y
ACCESS GRANTED
226
RETURN
234

FIG. 11


240
START
242
O.S. RECEIVES COMMAND FROM USER: DELETE XYZ
244
O.S. CHECKS: USER ALLOWED DEL COMMAND?
N
Y
246
LOAD DEL, FETCH ACCESS RIGHTS
ACCESS RIGHTS MATCH CURRENT USER?
N
248
Y
MATCH: HOME DIRECTORY AND CURRENT USER?
N
250
Y
256
252
ACCESS GRANTED, EXECUTE COMMAND
ACCESS RIGHTS DENIED
254
RETURN

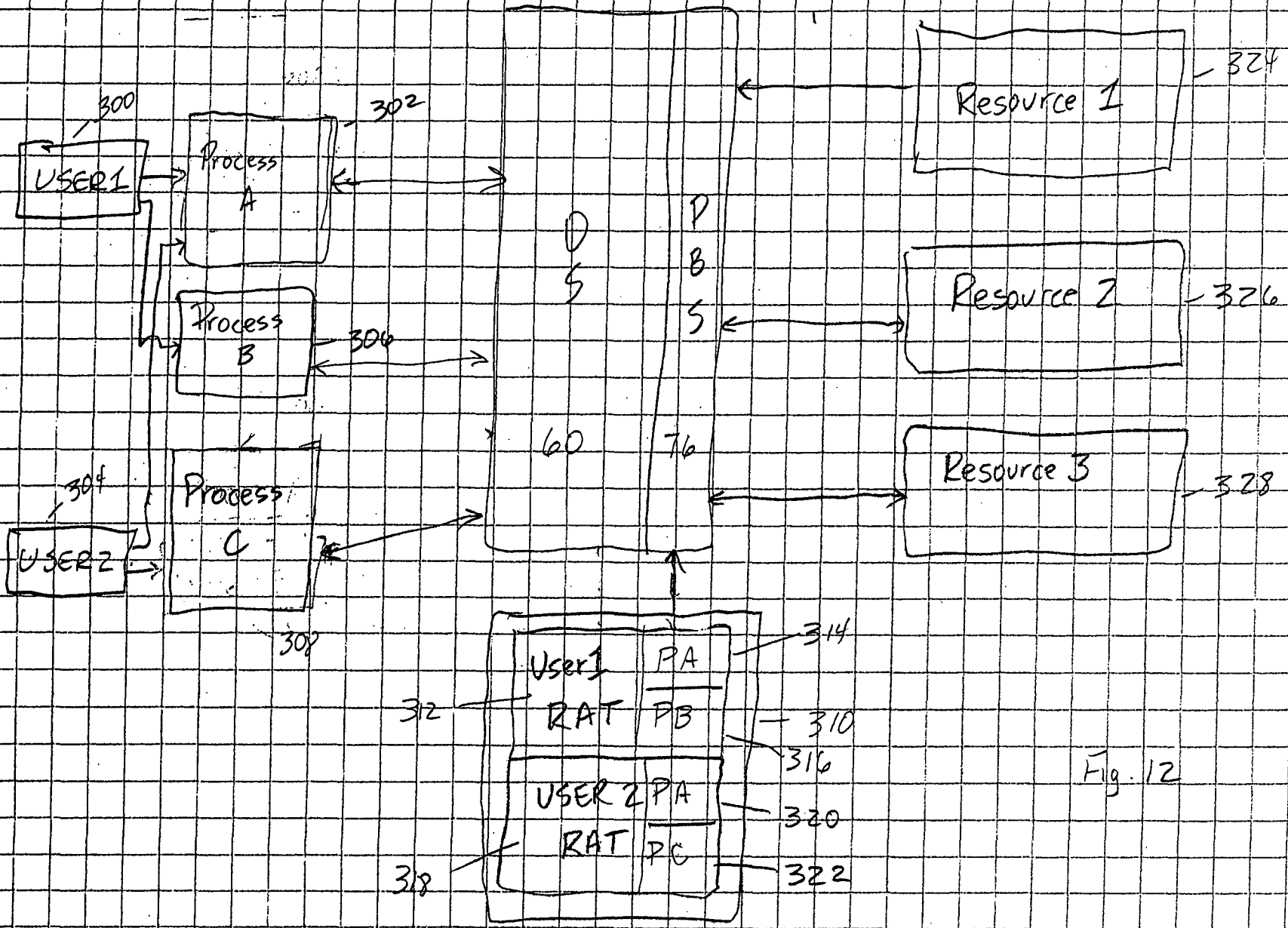

300
USER1
302
Process A
Process B
306
304
USER2
Process C
308
60
76
D
S
P
B
S
Resource 1
324
Resource 2
326
Resource 3
328
User1
PA
RAT
PB
312
314
310
316
USER 2
PA
RAT
PC
318
320
322

Fig. 12

Figure 13

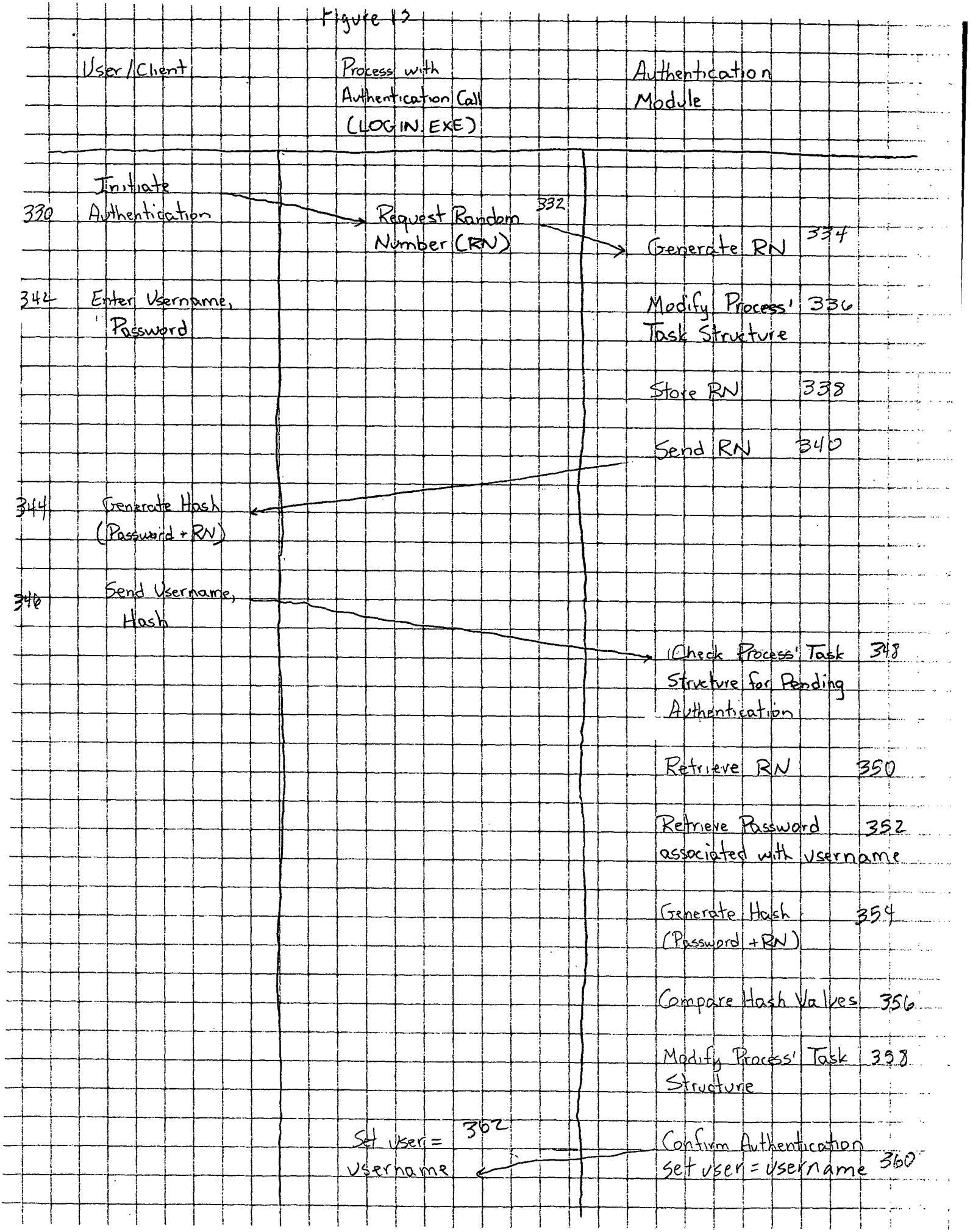

User/Client
Process with Authentication Call (LOGIN.EXE)
Authentication Module
330 Initiate Authentication
332 Request Random Number (RN)
334 Generate RN
336 Modify Process' Task Structure
338 Store RN
340 Send RN
342 Enter Username, Password
344 Generate Hash (Password + RN)
346 Send Username, Hash
348 Check Process' Task Structure for Pending Authentication
350 Retrieve RN
352 Retrieve Password associated with username
354 Generate Hash (Password + RN)
356 Compare Hash Values
358 Modify Process' Task Structure
360 Confirm Authentication set user = username
362 Set user = username

Figure 14

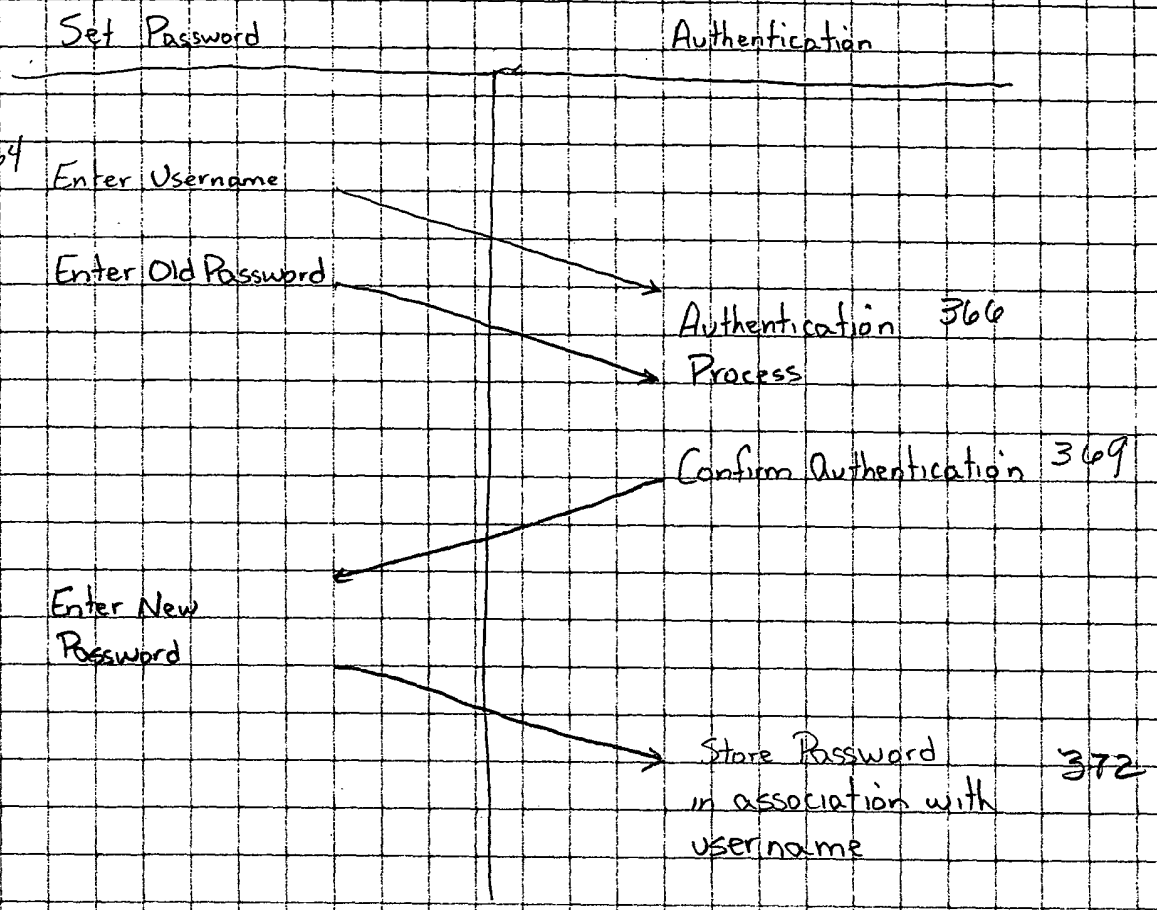

Set Password
Authentication
364
Enter Username
368
Enter Old Password
Authentication Process
366
Confirm Authentication
369
370
Enter New Password
Store Password in association with username
372

Fig. 15

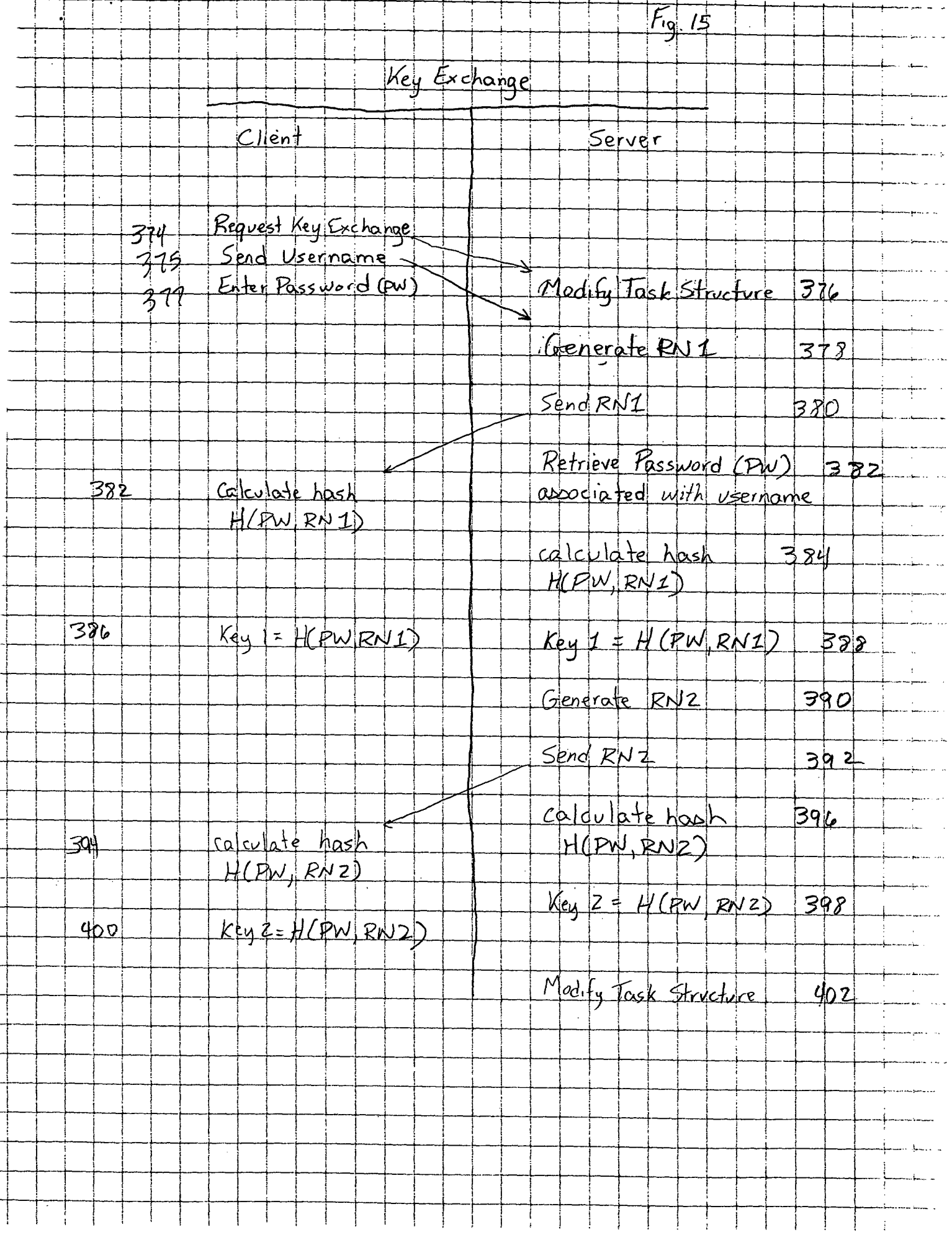

Key Exchange
Client
Server
374 Request Key Exchange
375 Send Username
379 Enter Password (PW)
376 Modify Task Structure
378 Generate RN1
380 Send RN1
382 Retrieve Password (PW) associated with username
382 Calculate hash H(PW, RN1)
384 calculate hash H(PW, RN1)
386 Key 1 = H(PW, RN1)
388 Key 1 = H(PW, RN1)
390 Generate RN2
392 Send RN2
394 calculate hash H(PW, RN2)
396 calculate hash H(PW, RN2)
400 Key 2 = H(PW, RN2)
398 Key 2 = H(PW, RN2)
402 Modify Task Structure

Fig 16

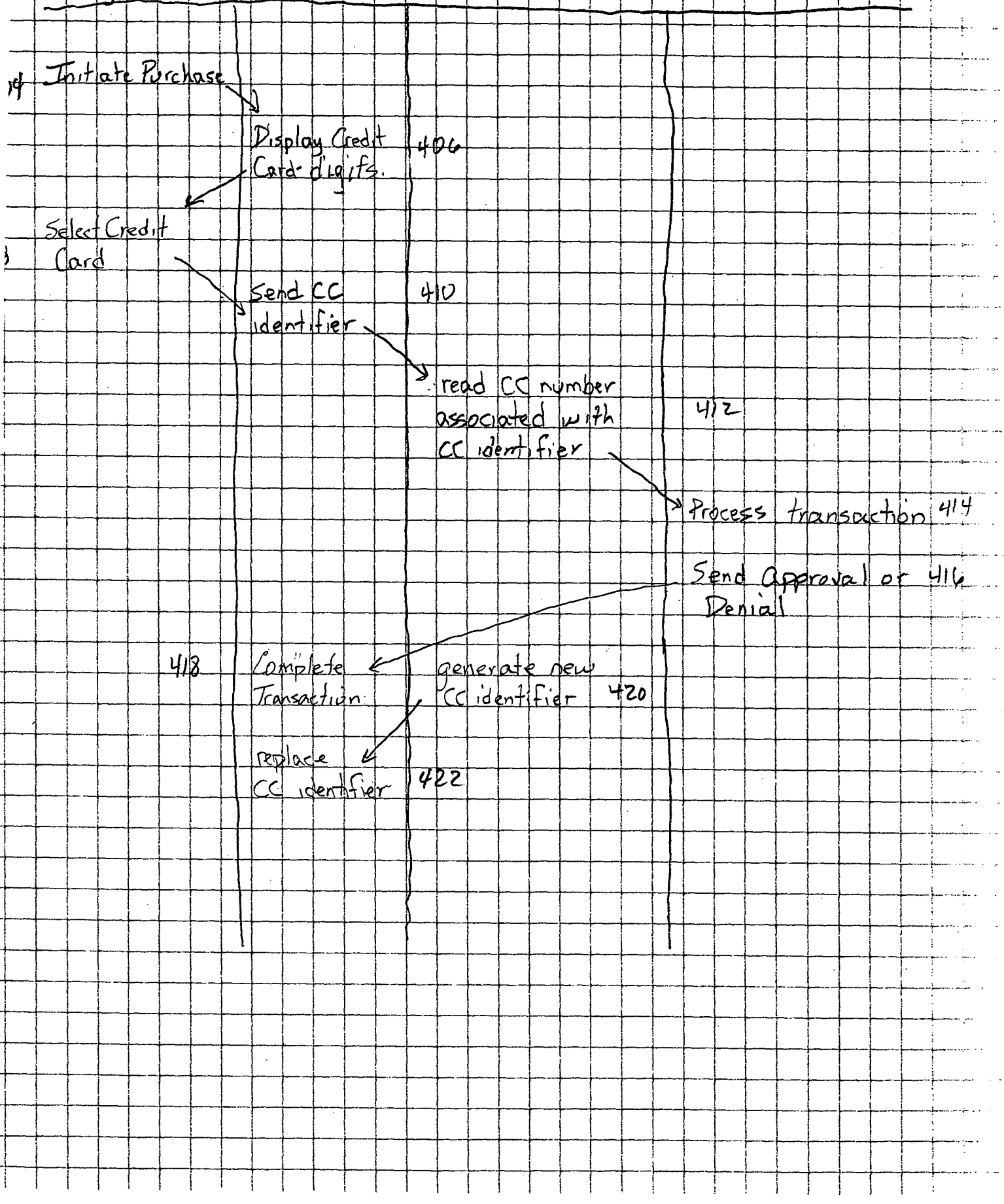
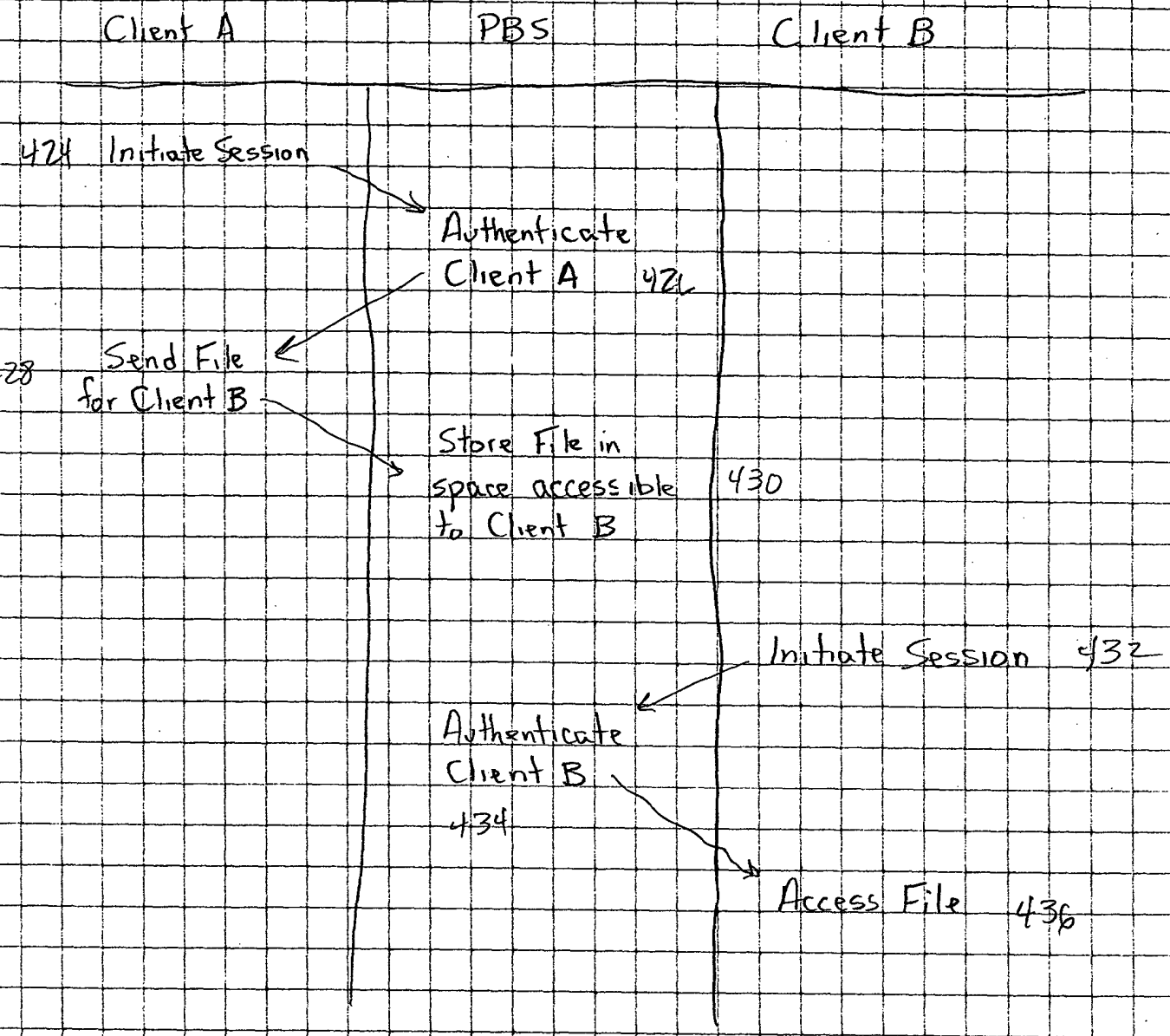

Buyer
POS
PBS Server
Financial Server
Initiate Purchase
Display Credit Card digits.
406
Select Credit Card
Send CC identifier
410
read CC number associated with CC identifier
412
Process transaction
414
Send Approval or Denial
416
418
Complete Transaction
generate new CC identifier
420
replace CC identifier
422

Fig 17


Client A
PBS
Client B
424 Initiate Session
Authenticate Client A 426
428 Send File for Client B
Store File in space accessible to Client B 430
Initiate Session 432
Authenticate Client B 434
Access File 436

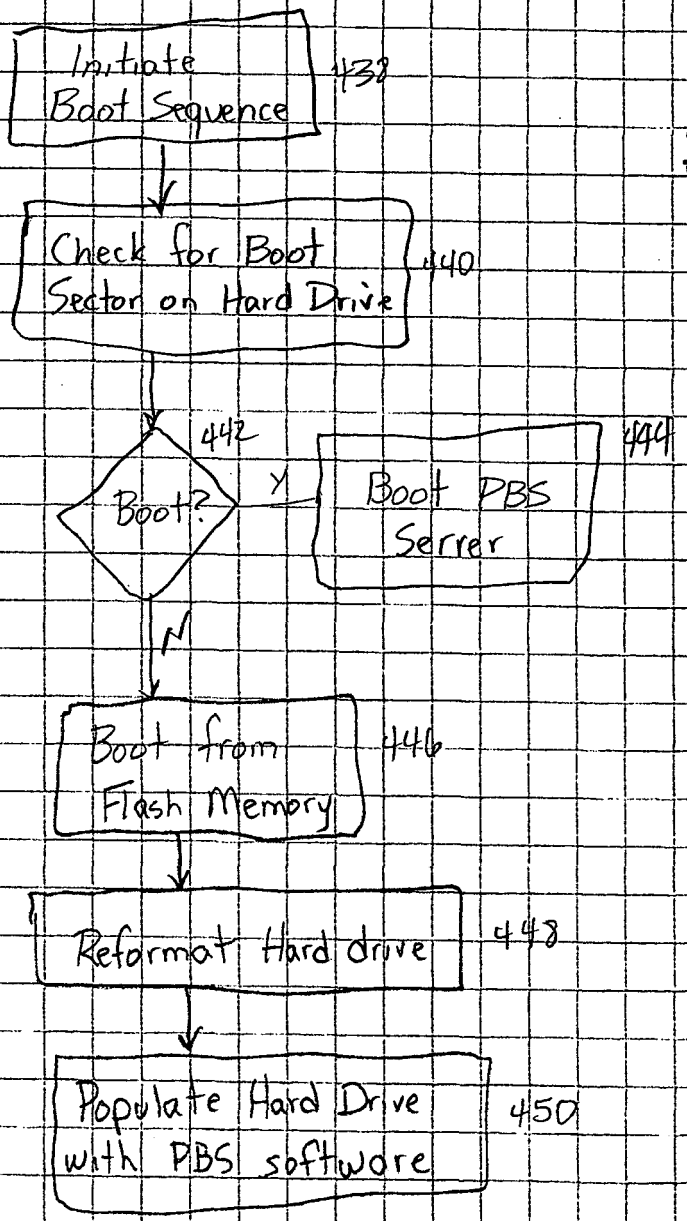

Initiate Boot Sequence
438
Check for Boot Sector on Hard Drive
440
442
Boot?
Y
Boot PBS Server
444
N
Boot from Flash Memory
446
Reformat Hard drive
448
Populate Hard Drive with PBS software
450

Fig 18